

IAP9 Rec'd PCT/PTO 19 DEC 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|-----------------------------------|---|-------------------|
| In re Patent Application of |) | |
| Marc JOYE |) | Group Art Unit: |
| Application No.: Unassigned |) | Examiner: |
| Filed: December 1, 2005 |) | Confirmation No.: |
| For: METHOD FOR COUNTERMEASURING) |) | |
| BY MASKING THE ACCUMULATOR IN) |) | |
| AN ELECTRONIC COMPONENT |) | |
| WHILE USING A PUBLIC KEY |) | |
| CRYPTOGRAPHIC ALGORITHM |) | |

FIRST INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure as set forth in 37 C.F.R. § 1.56, the accompanying information is being submitted in accordance with 37 C.F.R. §§ 1.97 and 1.98.

The listed documents were cited in the International Search Report in the corresponding PCT application.

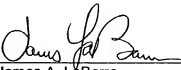
To assist the Examiner, the documents are listed on the attached form PTO-1449. However, copies of the documents are not provided as it is understood that they have already been transmitted by the International Bureau. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date December 17, 2005

By:


James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, VA 22313-1404
(703) 836-6620

10/561234

IPAP Doc 1 DCT/PTO 19 DEC 2009

Substitute for form 1449A/PTO & 1449B/PTO

FIRST INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

| | |
|-------------------------------|-------------------|
| Application Number | |
| Filing Date | December 16, 2005 |
| First Named Inventor | Marc JOYE |
| Examiner Name | |
| Attorney Docket Number | 032326-315 |

U.S. PATENT DOCUMENTS

| Examiner Initials | Document Number | Kind Code (if known) | Name of Patentee or Applicant of Cited Document | Issue/Publication Date (MM-DD-YYYY) |
|-------------------|-----------------|----------------------|---|-------------------------------------|
| /K.A./ | US/2003/0079139 | A1 | Drexler et al. | 04-24-2003 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

FOREIGN PATENT DOCUMENTS

| Examiner Initials | Document Number | Kind Code (if known) | Country | Date of Publication (MM-DD-YYYY) | STATUS | | | | | | |
|-------------------|-----------------|----------------------|---------|----------------------------------|-------------|---------------------|---------|--------------------|---------------|------|----------------|
| | | | | | Translation | Partial Translation | Summary | Eng. Lang. Summary | Search Report | IPER | Abstract Spec. |
| /K.A./ | *02/088934 | A1 | WIPO | 11-07-2002 | | | | | X | | |
| /K.A./ | *EP 1 296 224 | A1 | Europe | 03-26-2003 | | | | | X | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

NON-PATENT LITERATURE DOCUMENTS

| Examiner Initials | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | | |
|--------------------|--|-----------------|------------|
| /K.A./ | P-Y LIARDET et al., Preventing SPA/DPA in ECC Systems Using the Jacobi Form, Cryptographic Hardware and Embedded Systems., 3 rd International Workshop, Ches 2001, Paris, France, May 14-16, 2001, Proceedings, Lecture Notes in Computer Science, May 14, 2001, pp. 391-401, vol. 2162, Springer, DE. | | |
| /K.A./ | ELENA TRICHINA et al., Implementation of Elliptic Curve Cryptography with Built-In Counter Measures against Side Channel Attacks, Cryptography Hardware and Embedded Systems – CHES 2002, 4 th International Workshop Revised Papers, Redwood Shores, CA, Aug. 13-15, 2003, pp. 98-113., Berlin, Germany. | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Examiner Signature | /Kaveh Abrishamkar/ | Date Considered | 09/05/2008 |

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with M.P.E.P. § 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.
Form Letters I